REMARKS

[0005] Applicant respectfully requests reconsideration and allowance of all of the claims of the application. The status of the claims is as follows:

- Claims 1, 3-9, 11-22 and 46-54 are currently pending
- Claims 2, 10, and 23-45 are canceled herein
- No claims are withdrawn herein
- Claims 1, 3-6, 9, 11-14, 17-21 and 46-54 are amended herein
- No new claims are added herein

[0006] Claim 1 is amended to include subject matter from dependent claim 2. Claim 9 is amended to include subject matter from dependent claim 10. Support for the amendments to claims 1, 3-6, 9, 11-14, 17-21 and 46-54 is found in the specification at least at paragraphs [0073], [0076], [0084] and [0090].

Cited Documents

[0007] The following documents have been applied to reject one or more claims of the Application:

- **Felten et al., Felten** "Reading Between the Lines: Lessons from the SDMI Challenge" USENIX, August 13-17, 2001
- **Cox et al, Cox** "Some general methods for tampering with watermarks" IEEE, 1998, pages 1-15

Claims 1-22 and 46-54 Are Non-Obvious Over Felten in view of Cox

[0008] Claims 1-22 and 46-54 stand rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Felten in view of Cox. Applicant respectfully traverses the rejection.

Independent Claim 1

[0009] Applicant submits that the Office will be unable to make a *prima facie* showing that independent claim 1, as amended, is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **observing and determining a location in a processor-readable memory of a computer, where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream** for the watermark detector to perform detection thereon to determine if the stream has an embedded-signal therein;

[0010] Claim 1 recites in part, "observing and determining a location in a processor-readable memory of a computer, where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream." The Office cites Felten, (Abstract; 1. Introduction; 3.1 Attack and Analysis of Technology A; 5. Conclusion) as teaching this feature. (Office Action, page 4).

[0011] Felten describes, "The Secure Digital Music Initiative (SDMI) held a challenge to test the strength of four watermarking technologies." (Felten, Abstract). "SDMI announced a "public challenge" in which it invited members of the public to try to break certain data-encoding technologies that SDMI had developed." (Felten, 1. Introduction). Felton goes on to describe, "A reasonable first step in analyzing watermarked content

with original, unmarked samples is differencing the original and marked versions in some way. Initially, we used sample-by-sample differences in order to determine roughly what kinds of watermarking methods were taking place." (Felten, 3.1 Attack and Analysis of Technology A). "Each technology challenge described a specific goal (e.g., render undetectable a watermark from an audio track)." (Felten, 5. Conclusion).

[0012] It appears the Office is confusing watermarking technologies, watermark detection, watermark analysis, the breaking of watermarks and the rendering as undetectable a watermark from an audio track, as described by Felten, with the claimed "observing and determining a location in a processor-readable memory of a computer, where a...watermark detector...receives a subject input stream."

[0013] Nowhere does Felton disclose, teach or suggest, "observing and determining a location in a processor-readable memory of a computer, where a ..."watermark detector" receives a subject input stream." Instead, Felten is directed towards determining what kinds of watermarking methods are being used and testing the strength of watermarking technologies. Felten never mentions nor seems to even contemplate where the watermark detector resides in memory nor where, specifically in memory, that the detector receives the watermarked signal. Therefore, Felton fails to teach or suggest, "where..in memory..a watermark detector receives a subject input stream," as claim 1 recites.

[0014] Furthermore, during the in-person interview, the Examiner referred to section 6.1 of Cox (which was not relied upon in the rejections). In particular, the Examiner pointed to the second sentence of the first paragraph of that section of Cox: "Nevertheless, [the attacker] usually has access to a detector and the detector provides

information about whether a certain piece of content contains a watermark or not." It is the Examiner's position that this section, this text, and this phrase in particular "has access to the detector" teaches or discloses what is claimed here, esp. with regard to the claim language: "where..in memory..a watermark detector receives a subject input stream," as claim 1 recites.

[0015] Applicant respectfully disagreed and explained why at the in-person meeting. In short, that explanation is that Cox is, at most, suggesting and teaching that knowing the behavior of the detector will help guide the attacker in identifying and isolating the watermark in the incoming signal. This will allow the attacker to be more successful in removing the watermark from the signal. The first sentence of the second paragraph of section 6.1 of Cox says this: "The aim of the attack is to experimentally deduce the behavior of the detector, and to exploit this knowledge to ensure that a particular [watermarked signal] does not trigger the detector."

[0016] Applicant submits that knowing the behavior of the detector does not require that one know, "where…watermark detector…receives a subject input stream," as claim 1 recites. Furthermore, the Office has not provided any objective evidence to show that "knowing the behavior of the detector" as taught by Cox is equivalent to knowing "where…watermark detector…receives a subject input stream," as claim 1 recites.

[0017] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Dependent Claims 2-8

[0018] Claims 2-8 ultimately depend from independent claim 1. As discussed above, claim 1 is allowable over the cited documents. Therefore, claims 2-8 are also allowable over the cited documents of record for at least their dependency from an allowable base claim. These claims may also be allowable for the additional features that each recites.

Independent Claim 9

[0019] Applicant submits that the Office will be unable to make a *prima facie* showing that amended independent claim 9 is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **observing and determining a location in a processor-readable memory of a computer where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream** for the watermark to perform detection thereon to determine if the stream has an embedded-signal therein;

[0020] Claim 9 recites in part, "observing and determining a location in a processor-readable memory of a computer where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream." The Office cites Felten, (Abstract; 1. Introduction; 3.1 Attack and Analysis of Technology A; 5. Conclusion) as teaching this element. (Office Action, page 4). Felten describes, "a reasonable first step in analyzing watermarked content with original, unmarked samples is differencing the original and marked versions in some way. Initially, we used sample-by-sample differences in order to determine roughly what kinds of watermarking methods were

taking place." (Felten, 3.1 Attack and Analysis of Technology A). Felton goes on to describe, "Each technology challenge described a specific goal (e.g., render undetectable a watermark from an audio track)." (Felten, 5. Conclusion).

[0021] It appears the Office is equating the, "analyzing watermarked content" and "determin(ing) roughly what kinds of watermarking methods were taking place," as described by Felten, with the "observing and determining a location in a processor-readable memory of a computer, where a...watermark detector...receives a subject input stream," as claim 9 is amended to recite in part. Nowhere does Felton disclose, teach or suggest, "observing and determining a location in a processor-readable memory of a computer, where a...watermark detector...receives a subject input stream." Instead, Felten is directed towards determining what kinds of watermarking methods are being used in order to test the strength of watermarking technologies. Felten never mentions nor seems to even contemplate where the watermark detector resides in memory nor where, specifically in memory, that the detector receives the watermarked signal. Therefore, Felton fails to teach or suggest, "where a...watermark detector...receives a subject input stream," as claim 9 recites.

[0022] Furthermore, during the in-person interview, the Examiner referred to section 6.1 of Cox (which was not relied upon in the rejections). In particular, the Examiner pointed to the second sentence of the first paragraph of that section of Cox: "Nevertheless, [the attacker] usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not." It is the Examiner's position that this section, this text, and this phrase in particular "has access to the detector" teaches or discloses what is claimed here, esp. with regard to

the claim language: "a location in a processor-readable memory of a computer where a...watermark detector...receives a subject input stream," as claim 9 recites.

[0023] Applicant respectfully disagreed and explained why at the in-person meeting. In short, that explanation is that Cox is, at most, suggesting and teaching that knowing the behavior of the detector will help guide the attacker in identifying and isolating the watermark in the incoming signal. This will allow the attacker to be more successful in removing the watermark from the signal. The first sentence of the second paragraph of section 6.1 of Cox says this: "The aim of the attack is to experimentally deduce the behavior of the detector, and to exploit this knowledge to ensure that a particular [watermarked signal] does not trigger the detector."

[0024] Applicant submits that knowing the behavior of the detector does not require that one know, "where a...watermark detector...receives a subject input stream," as claim 9 recites. Furthermore, the Office has not provided any objective evidence to show that "knowing the behavior of the detector" as taught by Cox is equivalent to knowing "where a...watermark detector...receives a subject input stream," as claim 9 recites.

[0025] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Dependent Claims 10-16

[0026] Claims 10-16 ultimately depend from independent claim 9. As discussed above, claim 9 is allowable over the cited documents. Therefore, claims 10-16 are also

allowable over the cited documents of record for at least their dependency from an allowable base claim. These claims may also be allowable for the additional features that each recites.

Independent Claim 17

[0027] Applicant submits that the Office will be unable to make a *prima facie* showing that independent claim 17, as amended, is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **a memory-location determiner ("watermark-detector detector") configured to determine where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform detection thereon** to determine if the stream has an embedded-signal therein;

[0028] Claim 17 is amended to recite in part, "a memory-location determiner ("watermark-detector detector") configured to determine where a dynamic embedded-signal detection program module ("watermark detector") receives a subject input stream for the watermark detector to perform detection thereon." The Office cites Felten, (Abstract; 1. Introduction; 3.1 Attack and Analysis of Technology A; 5. Conclusion) as teaching this element. (Office Action, page 4). Felten describes, "each technology challenge described a specific goal (e.g., render undetectable a watermark from an audio track)." (Felten, 5. Conclusion).

[0029] The "memory-location determiner ('watermark-detector detector')," as claim 17 is amended to recite, is "configured to determine where a...watermark detector...a subject input stream." This is not the same as Felton, who does not disclose, teach or suggest determining where in memory an input stream is received. The recitation of claim 17 is instead, "configured to determine where a...watermark detector...receives a subject input stream," in order "for the watermark detector to perform detection thereon to determine if the stream has an embedded-signal therein."

[0030] Felten never mentions nor seems to even contemplate where the watermark detector resides in memory nor where, specifically in memory, that the detector receives the watermarked signal. Therefore, Felton fails to teach or suggest "a memory-location determiner ("watermark-detector detector") configured to determine where a...watermark detector...receives a subject input stream," as claim 17 recites.

[0031] Furthermore, during the in-person interview, the Examiner referred to section 6.1 of Cox (which was not relied upon in the rejections). In particular, the Examiner pointed to the second sentence of the first paragraph of that section of Cox: "Nevertheless, [the attacker] usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not." It is the Examiner's position that this section, this text, and this phrase in particular "has access to the detector" teaches or discloses what is claimed here, esp. with regard to the claim language: "a memory-location determiner ('watermark-detector detector')," as claim 17 recites.

[0032] Applicant respectfully disagreed and explained why at the in-person meeting. In short, that explanation is that Cox is, at most, suggesting and teaching that knowing

the behavior of the detector will help guide the attacker in identifying and isolating the watermark in the incoming signal. This will allow the attacker to be more successful in removing the watermark from the signal. The first sentence of the second paragraph of section 6.1 of Cox says this: "The aim of the attack is to experimentally deduce the behavior of the detector, and to exploit this knowledge to ensure that a particular [watermarked signal] does not trigger the detector."

[0033] Applicant submits that knowing the behavior of the detector does not require that one know, "where a...watermark detector...receives a subject input stream," as claim 17 recites. Furthermore, the Office has not provided any objective evidence to show that "knowing the behavior of the detector" as taught by Cox is equivalent to knowing "where a...watermark detector...receives a subject input stream," as claim 17 recites.

[0034] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Dependent Claims 18-22

[0035] Claims 18-22 ultimately depend from independent claim 17. As discussed above, claim 17 is allowable over the cited documents. Therefore, claims 18-22 are also allowable over the cited documents of record for at least their dependency from an allowable base claim. These claims may also be allowable for the additional features that each recites.

Independent Claim 46

[0036] Applicant submits that the Office will be unable to make a *prima facie* showing that independent amended claim 46 is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **intervening with clear reception of the subject input stream**, thereby hindering watermark detection by the watermark detector, wherein the intervening comprises adjusting "play-rate" of the input stream

[0037] Claim 46 recites in part, "intervening with clear reception of the subject input stream." The Office states that, "Felten fails to explicitly disclose interfering with clear reception of the subject input stream, thereby hindering detection by the watermark detector, wherein the interfering comprises adjusting "play-rate" of the input stream. The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 6.)

[0038] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0039] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervening with clear reception of the subject input stream," as recited, in part, by amended claim 46. However, claim 46 goes on to recite, "thereby hindering watermark detection by the watermark detector wherein the intervening comprises adjusting 'play-rate' of the input stream." Nowhere does Cox disclose, teach or suggest "intervening comprises adjusting 'play-rate' of the input stream," as claim 46 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the very watermark that the content owner has embedded...he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "intervention" or "adjusting play-rate," as claim 46 recites in part, is disclosed in Cox.

[0040] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 47

[0041] Applicant submits that the Office will be unable to make a *prima facie* showing that independent claim 47, as amended, is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **intervening with clear reception of the subject incoming stream**, thereby hindering embedded-signal detection by the dynamic detector,

wherein the intervening comprises adjusting "consumption-rate" of the incoming stream.

[0042] Claim 47 recites in part, "intervening with clear reception of the subject incoming stream." The Office states that, "Felten fails to explicitly disclose interfering with clear reception of the subject incoming stream, thereby hindering embedded-signal detection by the dynamic detector, wherein the interfering comprises adjusting "consumption-rate" of the incoming stream. The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 7.)

[0043] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0044] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervening with clear reception of the subject incoming stream," as recited, in part, by amended claim 47. However, claim 47 goes on to recite, "thereby hindering embedded-signal detection by the dynamic detector wherein the

intervening comprises adjusting 'consumption-rate' of the incoming stream." Nowhere does Cox disclose, teach or suggest "intervening comprises adjusting 'consumption-rate' of the incoming stream," as claim 47 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the very watermark that the content owner has embedded…he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "intervening" or "adjusting consumption-rate," as claim 47 recites in part, is described by Cox.

[0045] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 48

[0046] Applicant submits that the Office will be unable to make a *prima facie* showing that amended independent claim 48 is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **a memory-location determiner ("watermark-detector detector") configured to determine where, in a memory, an embedded-signal detection program module ("detector") receives a subject input stream** for the detector to perform detection thereon to determine if the subject input stream has an embedded-signal therein and further configured to detect and observe the detector in a processor-readable memory of a computer to determine its location in such memory;

- **an intervention component configured to intervene with clear reception** of the subject input stream, thereby hindering watermark detection by the detector, wherein the intervening comprises adjusting an incoming rate for the input stream

[0047] Claim 48 recites in part, "a memory-location determiner ("watermark-detector detector") configured to determine where, in a memory, an embedded-signal detection program module ("detector") receives a subject input stream." The Office cites Felton, (Abstract; 1. Introduction; 3.1 Attack and Analysis of Technology A; and 5. Conclusion) as teaching this element. (Office Action, pages 7-8.) Felten describes, "a reasonable first step in analyzing watermarked content with original, unmarked samples is differencing the original and marked versions in some way. Initially, we used sample-by-sample differences in order to determine roughly what kinds of watermarking methods were taking place." (Felten, 3.1 Attack and Analysis of Technology A).

[0048] The "memory-location determiner ('watermark-detector detector')," as claim 48 is amended to recite, is "configured to determine where, in a memory, an embedded-signal detection program module receives a subject input stream." This is not the same as Felton, whose goal is to render a watermark undetectable. The recitation of claim 48 is instead, "configured to determine where, in a memory, an embedded-signal detection program module ('detector') receives a subject input stream," in order "for the detector to perform detection thereon to determine if the stream has an embedded-signal therein." Felton does not teach or suggest, "determining where, in a memory..a detector receives a subject input stream," as claim 48 recites.

[0049] Claim 48 goes on to recite in part, "an intervention component configured to intervene with clear reception." The Office states that Felten fails to explicitly disclose

an interferer configured to interfere with clear reception of the subject input stream, thereby hindering detection by the detector, wherein the interfering comprising adjusting the incoming rate for the input stream." (Office Action, page 8). The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 8.)

[0050] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0051] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervention component configured to intervene with clear reception of the subject input stream," as recited, in part, by amended claim 48. However, claim 48 goes on to recite in part, "thereby hindering watermark detection by the detector wherein the intervening comprises adjusting an incoming rate for the input stream." Nowhere does Cox disclose, teach or suggest "intervening comprises adjusting an incoming rate for the input stream," as claim 48 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the

very watermark that the content owner has embedded…he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "intervening" or "adjusting an incoming rate" as claim 48 recites in part, is taught by Cox.

[0052] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 49

[0053] Applicant submits that the Office will be unable to make a *prima facie* showing that independent claim 49, as amended, is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector,** wherein the intervening comprises introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal.

[0054] Claim 49 recites in part, "intervening with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector." The Office states that Felten fails to explicitly disclose interfering with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector, wherein the interfering comprising introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal." (Office Action, page 9). The Office

cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 9.)

[0055] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0056] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervening with clear reception of the subject input stream," as recited, in part, by amended claim 49. However, claim 49 goes on to recite, "thereby hindering watermark detection by the watermark detector wherein the intervening comprises introducing a countersignal." Nowhere does Cox disclose, teach or suggest "intervening comprises introducing a countersignal," as claim 49 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the very watermark that the content owner has embedded…he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "intervening" or "introducing a countersignal," as claim 49 recites in part, is suggested by Cox.

[0057] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 50

[0058] Applicant submits that the Office will be unable to make a *prima facie* showing that amended independent claim 50 is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **intervening with clear reception of the subject incoming stream, thereby hindering detection by the dynamic detector**, wherein the intervening comprises modifying the reception by introduction of a noise countersignal into the incoming stream.

[0059] Claim 50 recites in part, "intervening with clear reception of the subject incoming stream, thereby hindering detection by the dynamic detector." The Office states that Felten fails to explicitly disclose interfering with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector, wherein the interfering comprising introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal." (Office Action, page 9). The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 9.)

[0060] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is

completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0061] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervening with clear reception of the subject incoming stream," as recited, in part, by amended claim 50. However, claim 50 goes on to recite, "thereby hindering detection by the dynamic detector wherein the intervening comprises modifying the reception by introduction of a noise countersignal into the incoming stream." Nowhere does Cox disclose, teach or suggest "intervening comprises modifying the reception by introduction of a noise countersignal into the incoming stream," as claim 50 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the very watermark that the content owner has embedded…he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "intervening" or "modifying the reception by introduction of a noise countersignal," as claim 50 recites in part, is disclosed by Cox.

[0062] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 51

[0063] Applicant submits that the Office will be unable to make a *prima facie* showing that independent claim 51, as amended, is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **a memory-location determiner ("watermark-detector detector") configured to determine a location where, in a memory, an embedded-signal detection program module ("detector") receives a subject incoming stream for the detector to perform detection thereon** to determine if the incoming stream has an embedded-signal therein;
- **an intervention component configured to intervene with clear reception of the subject incoming stream**, thereby hindering detection by the detector, wherein the intervention component is further configured to modify the reception by introducing a countersignal into the incoming stream **at the location in memory determined to be where the subject incoming stream is being received by the detector**.

[0064] Claim 51 recites in part, "a memory-location determiner ("watermark-detector detector") configured to determine a location where, in a memory, an embedded-signal detection program module ("detector") receives a subject incoming stream for the detector to perform detection thereon." The Office cites Felten, (Abstract; 1. Introduction; 3.1 Attack and Analysis of Technology A; and 5. Conclusion) as teaching this element. (Office Action, pages 8-9.) Felten describes, "SDMI announced a "public

challenge" in which it invited members of the public to try to break certain data-encoding technologies that SDMI had developed." (Felten, 1. Introduction).

[0065] The "memory-location determiner ('watermark-detector detector')," as claim 51 is amended to recite, is "configured to determine a location where, in a memory, an embedded-signal detection program module ('detector') receives a subject incoming stream." This is not the same as Felton, whose goal is to render a watermark undetectable. The recitation of claim 51 is instead, "configured to determine a location where, in a memory, an embedded-signal detection program module ('detector') receives a subject incoming stream," in order "for the detector to perform detection thereon to determine if the incoming stream has an embedded-signal therein." Felton does not teach or suggest, "determining a location where, in a memory..a detector receives a subject input stream," as claim 51 recites.

[0066] Claim 51 goes on to recite in part, "an intervention component configured to intervene with clear reception of the subject incoming stream." The Office states that Felten fails to explicitly disclose interfering with clear reception of the subject input stream, thereby hindering watermark detection by the watermark detector, wherein the interfering comprising introducing a countersignal, the countersignal modifying the reception by introducing a noise countersignal." (Office Action, page 9). The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 9.)

[0067] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is

completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0068] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervention component configured to intervene with clear reception of the subject input stream," as recited, in part, by amended claim 51. However, claim 51 goes on to recite in part, "thereby hindering detection by the detector wherein the intervention component is further configured to modify the reception by introducing a countersignal into the incoming stream at the location in memory determined to be where the subject incoming stream is being received by the detector." Nowhere does Cox disclose, teach or suggest "modify the reception…at the location in memory determined to be where the subject incoming stream is being received by the detector," as claim 51 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the very watermark that the content owner has embedded…he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "watermark-detector detector" or "modify(ing) the reception…at the location in memory determined to be where the subject incoming stream is being received by the detector" as claim 51 is amended to recite in part, is taught by Cox.

[0069] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 52

[0070] Applicant submits that the Office will be unable to make a *prima facie* showing that amended independent claim 52 is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **intervening with clear reception of the subject input stream,** thereby hindering watermark detection by the watermark detector; and
- **maintaining the intervening while the subject input stream is being played.**

[0071] Claim 52 recites in part, "intervening with clear reception of the subject input stream." The Office states that, "Felten fails to explicitly disclose interfering with clear reception of the subject incoming stream, thereby hindering embedded-signal detection by the dynamic detector, wherein the interfering comprises adjusting "consumption-rate" of the incoming stream. The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 7.)

[0072] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the

watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0073] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervening with clear reception of the subject input stream," as recited, in part, by amended claim 52. However, claim 52 goes on to recite, "thereby hindering watermark detection by the watermark detector." Nowhere does Cox disclose, teach or suggest "hindering watermark detection by the watermark detector," as claim 52 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the very watermark that the content owner has embedded...he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "intervening" or "hindering watermark detection," as claim 52 recites in part, is suggested by Cox.

Claim 52 goes on to recite in part, "maintaining the intervening while the subject input stream is being played." Applicant respectfully points out that the Office fails to address this clause of claim 52, with particularity, in the Final Office Action dated 09/30/2009. However, even if the rejection was based upon the cited documents of Cox or Felten, nowhere does Cox or Felton disclose, teach or suggest, "determining where, in a memory, a...watermark detector...receives a subject input stream" or "maintaining the intervening while the subject input stream is being played." Instead, Felton's goal

merely wants to render a watermark undetectable and Cox discusses to what extent a watermark can be resistant to tampering and describes a variety of possible attacks.

[0074] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 53

[0075] Applicant submits that the Office will be unable to make a *prima facie* showing that independent claim 53, as amended, is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this claim, as amended (with emphasis added):

- **intervening with clear reception of the subject incoming stream**, thereby hindering detection by the dynamic detector; and
- **maintaining the intervening while the incoming stream is being presented.**

[0076] Claim 53 recites in part, "intervening with clear reception of the subject incoming stream." The Office states that, "Felten fails to explicitly disclose interfering with clear reception of the subject input stream, thereby hindering detection by the watermark detector, wherein the interfering comprises adjusting "play-rate" of the input stream. The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 6.)

[0077] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is

completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0078] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervening with clear reception of the subject incoming stream," as recited, in part, by amended claim 53. However, claim 53 goes on to recite, "thereby hindering detection by the dynamic detector." Nowhere does Cox disclose, teach or suggest "intervening with clear reception of the subject incoming stream, thereby hindering detection by the dynamic detector," as claim 53 recites. Instead, Cox is directed toward removal of the watermark, or if "an attacker may not wish to remove the very watermark that the content owner has embedded…he only desires to extract a pattern that cancels the effect that the present watermark has on the detector." (Cox, 6.1). In either case, no "intervening" or "hindering detection by the dynamic detector," as claim 53 recites in part, is described by Cox.

[0079] Claim 53 goes on to recite in part, "maintaining the intervening while the subject input stream is being presented." Applicant respectfully points out that the Office fails to address clause of claim 53, with particularity, in the Final Office Action dated 09/30/2009.

[0080] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Independent Claim 54

[0081] Applicant submits that the Office will be unable to make a *prima facie* showing that amended independent claim 54 is obvious in view of the combination Felten and Cox. Applicant submits that the combination of Felten and Cox does not teach or suggest at least the following features of this amended claim (with emphasis added):

- **a memory-location determiner ("watermark-detector detector") configured to detect and observe a dynamic watermark detection program module ("watermark detector")** in the processor-readable memory of a computer to detect and determine the location of the watermark detector in such memory, **the watermark-detector detector being further configured to detect and determine where, in the processor-readable memory, the watermark detector receives a subject input stream** for the watermark detector to perform watermark detection thereon to determine if the subject input stream has a watermark therein;
- **an intervention component configured to intervene with clear reception of the subject incoming stream by the watermark detector**, thereby hindering detection by the watermark detector,
- **the intervention component being further configured to maintain intervention while the subject input stream is being consumed by the watermark detector.**

[0082] Claim 54, as amended, recites in part, "a memory-location determiner ("watermark-detector detector") configured to detect and observe a dynamic watermark

detection program module ('watermark detector')." Amended clam 54 goes on to recite in part, "the watermark-detector detector being further configured to detect and determine where, in the processor-readable memory, the watermark detector receives a subject input stream." The Office cites Felten, (Abstract; 1. Introduction; 3.1 Attack and Analysis of Technology A; and 5. Conclusion) as teaching this element. (Office Action, pages 6-7).

[0083] Felten describes, "The Secure Digital Music Initiative (SDMI) held a challenge to test the strength of four watermarking technologies." (Felten, Abstract). "SDMI announced a "public challenge" in which it invited members of the public to try to break certain data-encoding technologies that SDMI had developed." (Felten, 1. Introduction). "A reasonable first step in analyzing watermarked content with original, unmarked samples is differencing the original and marked versions in some way. Initially, we used sample-by-sample differences in order to determine roughly what kinds of watermarking methods were taking place." (Felten, 3.1 Attack and Analysis of Technology A). "Each technology challenge described a specific goal (e.g., render undetectable a watermark from an audio track)." (Felten, 5. Conclusion).

[0084] It appears the Office is confusing watermarking technologies, watermark detection, watermark analysis, the breaking of watermarks and the rendering as undetectable a watermark from an audio track, as described by Felten, with the recitations of claim 54. Claim 54 is amended to draw further distinction between the recitations of claim 54 and the teachings of Felten.

[0085] Claim 54 recites in part, "a memory-location determiner ('watermark-detector detector')." And this watermark-detector detector is "configured to detect and observe a

dynamic watermark detection program module." One may ask, "Why?" "For what purpose?" And the answer to such question is also found in claim 54 which goes on to recite, "the watermark-detector detector...detect(s) and determine where, in the processor-readable memory, the watermark detector receives a subject input stream."

[0086] "So?" one might ask, "To what end?" Claim 54, as amended, answers these questions as it goes on to recite in part, "an intervention component configured to intervene with clear reception of the subject incoming stream by the watermark detector...the intervention component being further configured to maintain intervention while the subject input stream is being consumed by the watermark detector."

[0087] The Office states that, "Felten fails to explicitly disclose interfering with clear reception of the subject incoming stream, thereby hindering embedded-signal detection by the dynamic detector, wherein the interfering comprises adjusting "consumption-rate" of the incoming stream. The Office cites Cox, (5. Signal Transformation and 6. Intentional attacks) as teaching this element. (Office Action, page 7).

[0088] Cox states, "there are a number of common signal transformations that a watermark should survive, e.g. affine transformations, compression/re-compression, and noise. In some circumstances, it may be possible to design a watermark that is completely invariant to a particular transformation." (Cox, 5 Signal Transformations). Cox goes on to describe, "an attacker may not have precise knowledge of the watermark. Nevertheless, he usually has access to a detector and the detector provides information about whether a certain piece of content contains a watermark or not. This information can be used to remove the watermark." (Cox, 6 Intentional attacks – 6.1 Exploiting the presence of a watermark detector device).

[0089] It would appear that the Office is confusing a "watermark that is completely invariant to a particular transformation" and the "removal of the watermark" as suggested by Cox, with the "intervention component configured to intervene," as recited, in part, by amended claim 54.

[0090] However, the "intervention component configured to intervene," as claim 54 recites in part, is "further configured to maintain intervention while the subject input." Applicant respectfully points out that the Office fails to address clause of claim 54, with particularity, in the Final Office Action dated 09/30/2009.

[0091] Consequently, the combination of Felten and Cox does not teach or suggest all of the elements and features of this claim. Accordingly, Applicant respectfully requests that the rejection of this claim be withdrawn.

Conclusion

[0092] For at least the foregoing reasons, all pending claims are in condition for allowance. Applicant respectfully requests reconsideration and prompt issuance of the application.

[0093] If any issues remain that would prevent allowance of this application, **Applicant requests that the Examiner contact the undersigned representative before issuing a subsequent Action.**

Respectfully Submitted,

Lee & Hayes, PLLC
Representative for Applicant

/kaseychristie40559/ Dated: 11-18-2009
Kasey C. Christie
(kasey@leehayes.com; 509-944-4732)
Registration No. 40,559